vanbreda
RISK & BENEFITS

# Cyberrisico’s en Verzekering

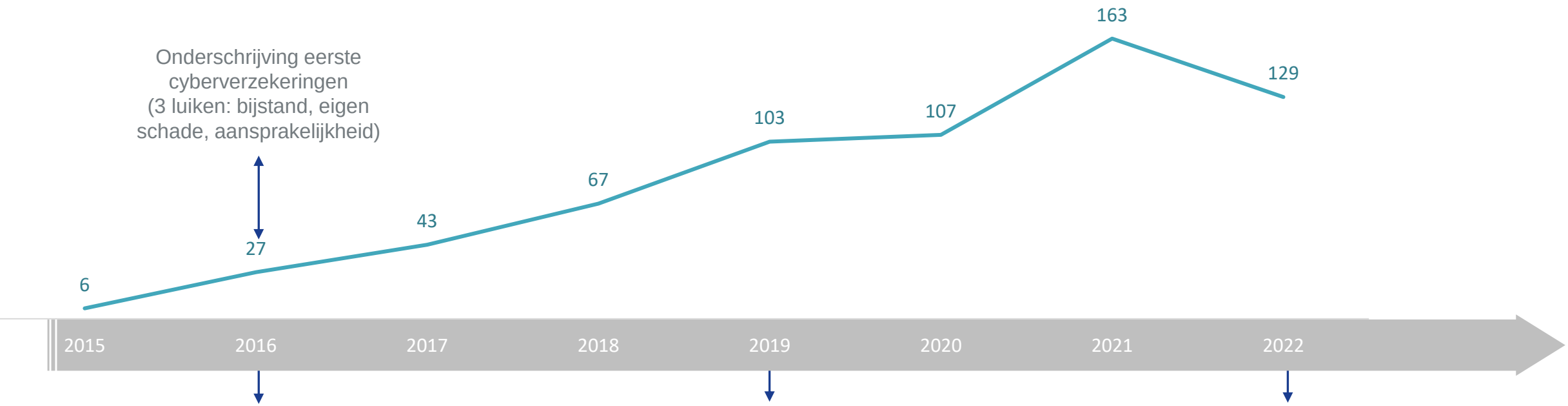
**Congres OVB De Magie van het Recht**
**26 april 2024**

/OVBCONGRES
DE MAGIE V/H RECHT
ELISABETH CENTER
ANTWERPEN

| Industry | Q1 Increase | Q2 Increase | Q3 Increase | Q4 Increase |
|---|---|---|---|---|
| Transportation, Logistics, and Storage | +80% | +33% | +50% | +33% |
| Telecommunications | +50% | +42% | +29% | -23% |
| Law Practices | +41% | +25% | +70% | -33% |
| Retail | +36% | +60% | +21% | -34% |
| Real Estate | +42% | +59% | +15% | -19% |
| Construction | +27% | +2% | +27% | -6% |

# Historiek cyberverzekeringen

**Evolutie aantal claims**




- Grote onderschrijvingsappetijt
- Veel verzekeraars
- Veel beschikbare capaciteit
- Weinig beveiligingsvereisten
- Ruime waarborgen
- Lage vrijstellingen
- Lage premies

- Onderschrijvingsappetijt neemt af
- Minder verzekeraars
- Beschikbare capaciteit daalt
- Beveiligingsvereisten toenemend belang
- Waarborgen worden beperkter
- Vrijstellingen verhoogd
- Premies stijgen

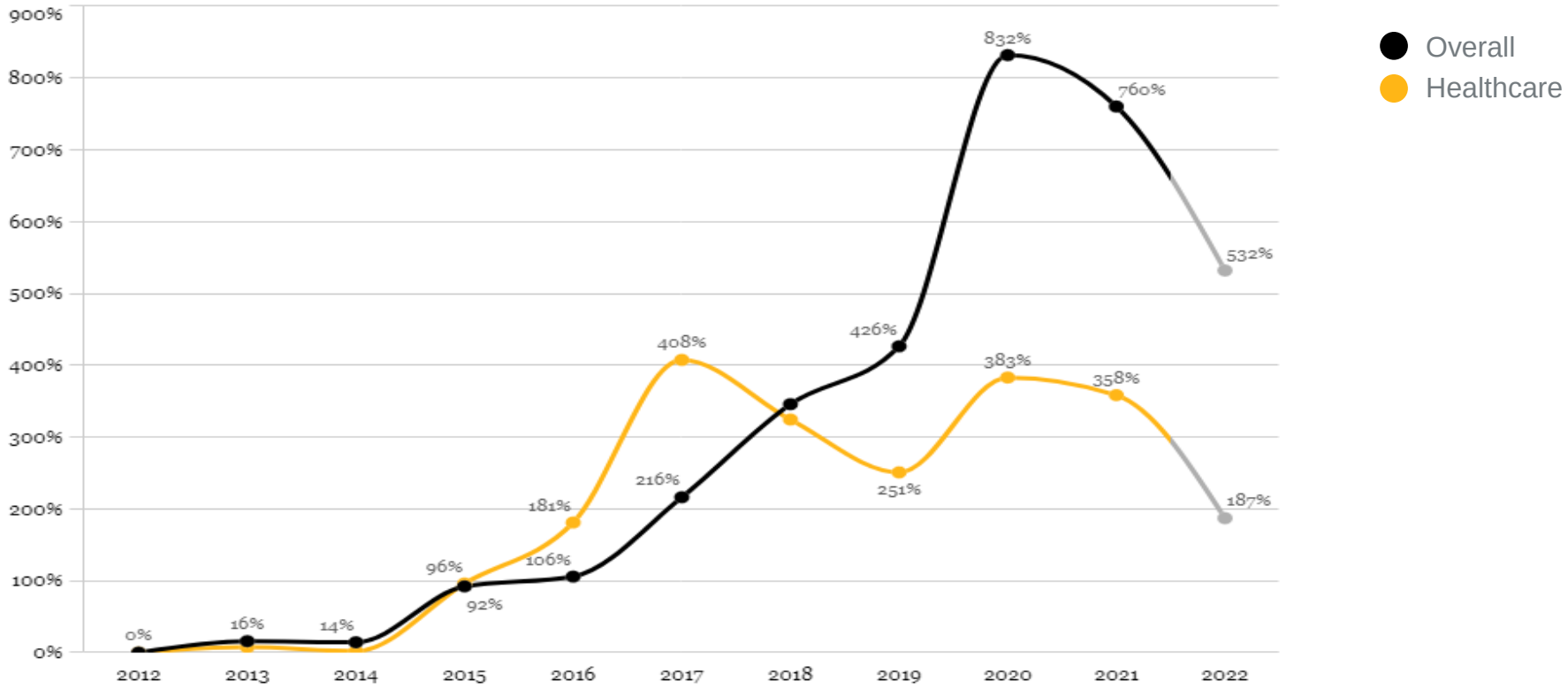
- Zeer moeizame onderschrijving
- Slechts 2 verzekeraars
- Zeer beperkte capaciteit
- Zeer strenge beveiligingsvereisten
- Strikte waarborgen
- Zeer hoge vrijstellingen
- Fors verhoogde premies

**Bron: AIG BELUX**

# Aantal incidenten

## Global Incident Growth Compared to 2012*

Global, Healthcare, All Revenu Sizes



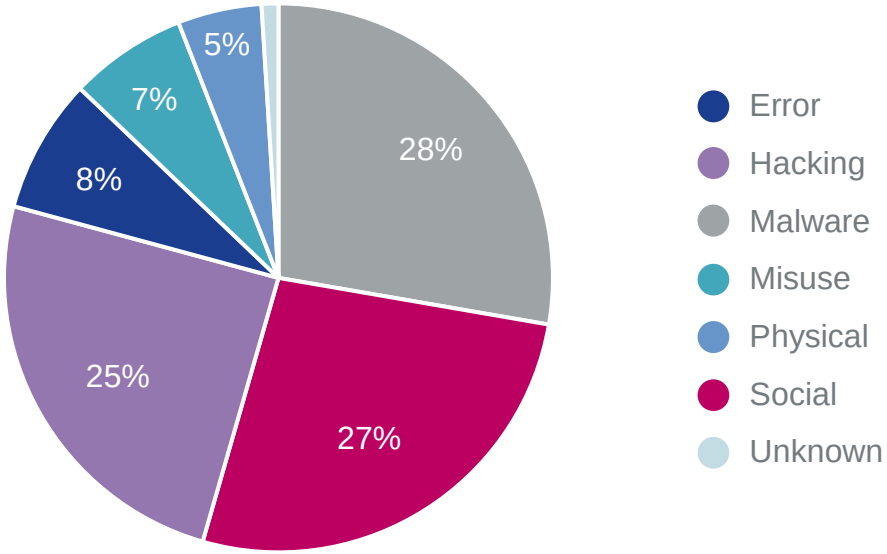

* Please note: This data is indexed against the base line year of 2012 and current year shown in grey is a projection.

Bron: Chubb

# Aard van de incidenten

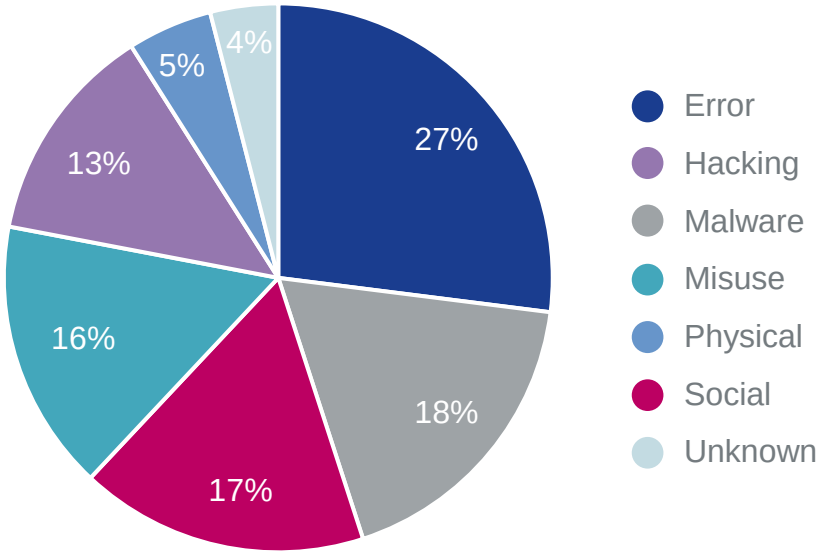
**Actions Causing Cyber Incidents – Last Complete Year**

Global, Healthcare and All Revenu Sizes




**Actions Causing Cyber Incidents – Last Five Complete Years**

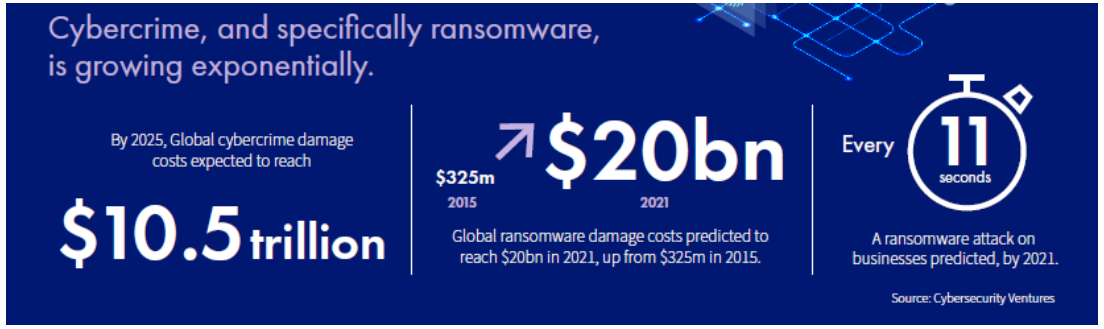
Global, Healthcare and All Revenu Sizes




**Bron: Chubb**

# Ernst van de incidenten


Network outages and business interruption are lasting longer. AIG observed a typical outage length of 7-10 days from global ransom and extortion claims




**Ransomware claims have increased significantly in frequency and severity in recent and continue to evolve**

**150%**
**Increase in frequency**
AIG has seen an increase of more than 150% in frequency of ransom and extortion claims notifications since 2018.

All sizes of company are impacted by ransomware, across all types of industries.

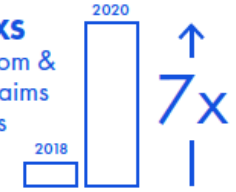

Ransom and extortion claims accounted for 1 in every 5 cyber claims in 2020, up from 1 in every 10 cyber claims in 2018.

Demand values can be in the tens of millions of dollars with payments varying depending on the characteristics of the attack.

**2x**

When data was exfiltrated prior to encryption, ransom and extortion claims costs were 2x higher.

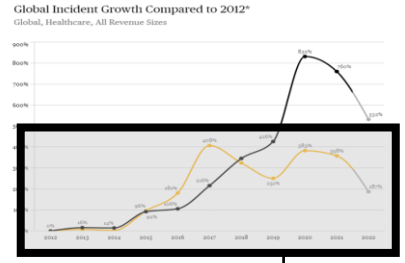
Increased **XS** policy ransom & extortion claims notifications in U.S.

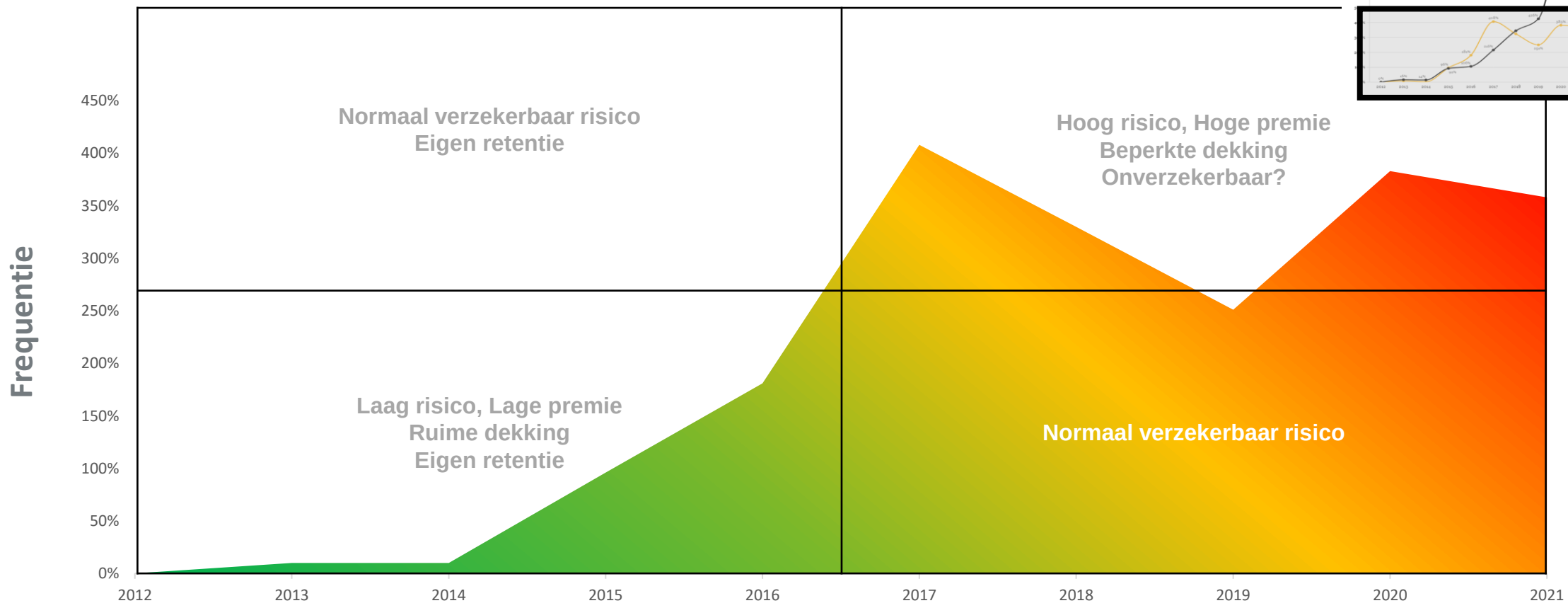



Losses may impact multiple coverage sections: extortion, event management, network interruption, security & privacy.

**Bron: AIG cyber claims analysis Q3 2020**

# Cyberverzekering : evolutie frequentie




Bron: Chubb Healthcare

# Verzekeringssector: Technische aanbevelingen

**Ransomware victims have similar deficiencies in control for managing ransomware risk.**

## Key controls:

- Use strong authentication controls for all administrative acces where possible, and deploy compensating controls where it's not.
- Deploy modern endpiont controls and timely remedaite vulnerabilities.
- Enable appropiate active directory controls and understand/verify your attack surface.

**Bron: AIG cyber claims analysis Q3 2020**

# Verzekeringssector: Red flags

- Sterke wachtwoorden
- Back-up beleid en –strategie (offline)
- MFA en extra MFA voor admin profiel
- Gescheiden netwerksegementen
- Third Party Management
- Veiligheidstraining gebruikers
- Business Continuity Plan & Disaster Recovery Plan actief en getest
- Scans van Active Directory en kwetsbaarheden

vanbreda

vanbreda
RISK & BENEFITS

# Datums van toetreding van de verschillende balies tot de cyberpolis OVB

- Balie Antwerpen, Gent, Dendermonde vanaf 6/6/2018
- Balie Turnhout vanaf 7/6/2018
- Balie Limburg vanaf 19/6/2018
- Balie Mechelen vanaf 20/6/2018
- Balie Oudenaarde vanaf 17/7/2018
- Balie Leuven vanaf 01/01/2019
- Balie West-Vlaanderen vanaf 22/04/2020

# Aantal dossiers

| Jaar | Aantal | Aangesloten advocaten |
|---|---|---|
| 2018 | 8 | 6.159 |
| 2019 | 10 | 6.175 |
| 2020 | 4 | 7.634 |
| 2021 | 12 | 7.696 |
| 2022 | 17 | 7.666 |
| 2023 | 6 | (7.666) |
| **Totaal** | **57** | |

# Reserve, betaald, totaal kost per jaar

| Jaar | Reserve | Betaald | Totaal kost |
|---|---|---|---|
| 2018 | 0 | 19.788,89 | 19.788,89 |
| 2019 | 0 | 118.394,76 | 118.394,76 |
| 2020 | 0 | 11.165,08 | 11.165,08 |
| 2021 | 0 | 67.035,87 | 67.035,87 |
| 2022 | 2.000 | 203.964,14 | 205.964,14 |
| 2023 | 55.348,46 | 78.628,52 | 133.976,98 |
| **Totaal** | **57.348,46** | **498.977,26** | **556.325,72** |

# Gemiddelde kost

| Jaar | Totale kost | Aantal | Gemiddelde kost |
|---|---|---|---|
| 2018 | 19.788,89 | 8 | 2473,61 |
| 2019 | 118.394,76 | 10 | 11.839,48 |
| 2020 | 11.165,08 | 4 | 2.791,27 |
| 2021 | 67.035,87 | 13 | 5.586,32 |
| 2022 | 205.964,14 | 17 | 12.115,54 |
| 2023 | 133.976,98 | 6 | 22.329,50 |
| **Totaal** | **556.325,72** | **57** | **9.760,10** |

# Omschrijving

| Omschrijving | Aantal | Reserve | Betaald | Totaal kost | Gemiddelde |
|---|---|---|---|---|---|
| Cybertheft (diefstal gelden via intrusie) | 9 | 21.528,00 | 253.247,60 | 274.775,60 | 30.530,62 |
| Hacking (ongeoorloofd binnedringen in een computersysteem) | 3 | 31.820,46 | 68.322,12 | 100.142,58 | 33.380,86 |
| Business email compromise (Phishing, hacking e-mail account) | 22 | 4.000,00 | 81.220,90 | 85.220,90 | 3.873,68 |
| Ransomware ( gijzelsoftware, chantagemiddel met vraag tot betalen losgeld) | 7 | 0,00 | 79.531,54 | 79.531,54 | 11.361,65 |
| Unauthorised use of picture | 1 | 0,00 | 7.216,50 | 7.216,50 | 7.216,50 |
| Cybertheft on personal accounts (ontvreemding gelden van persoonlijke rekening) | 1 | 0,00 | 3.869,98 | 3.869,98 | 38.69,98 |
| Sextorsion (seksuele afpersing op basis van bv geëxfiltreerde beelden) | 2 | 0,00 | 3.846,53 | 3.846,53 | 1.923,27 |
| Virus | 1 | 0,00 | 1.722,09 | 1.722,09 | 1.722,09 |
| CEO fraud (Frauduleus betalingsverzoek) | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Copywrite infringment (inbreuk op auteursrecht) | 2 | 0,00 | 0,00 | 0,00 | 0,00 |
| Cybertheft  probably within deductible | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Data breach : e-mails sent to incorrect adress (gegevenslek) | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Fraud via telephone | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Fraudulent SMS ITSME link | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Hacking with data breach and sextorsion by using exfiltrated data (zie voorgaande) | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| No info received | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| Spam e-mails | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| (blank) | 1 | 0,00 | 0,00 | 0,00 | 0,00 |
| **Totaal** | **57** | **57.348,46** | **498.977,26** | **556.325,72** | **9.760,10** |

# Business e-mail compromise

- Hacking e-mailaccount opgave foutief rekeningnummer.
- Phishing e-mailtoegang tot home banking account met intrusie.
- Phishing e-mail ING, daarna telefoon frauduleuse (medewerker) ING i.v.m. verdachte bewegingen op rekening, vraag gelden in veiligheid te brengen gevolg overschrijving naar buitenlandse rekening.
- Hacking e-mailaccount, e-mails verstuurd naar 3160 contacten, 2.000 EUR.
- Hacking e-mailaccount, e-mails verzonden naar contacten met vraag betaling 2.000 EUR, massaal inkomende telefoons met vraag correctheid factuur.

# Cybertheft

- Hacking app Belfius - bedragen overgemaakt.
- Hacking Office 365, hackers passen rekeningnummers aan op documenten van derden.
- Toegang tot bankapp na ontvangst valse mail Covid-vacinatie.
- Phishing e-mail gevolgd door fraudeleus telefoontje van fraude preventie ING, computer op afstand overgenomen en gelden ontvreemd.
- Phishing via Itsme e-mail, toegang tot systeem, gelden ontvreemd.
- Alias e-mailadres manager gebruikt om inkopen te laten doen.

# Ransomware

- Cyber attack, encryptie databestanden, betaling ransom.
- Cryptolocker, factuur eigen IT-partner betaald, geen ransom.

# Door verzekeraar opgelegde beveiligings-maatregelen

## Dekkingsvoorwaarden

De dekking van de huidige polis is cfr. Art. 65 Verzekeringswet enkel van toepassing indien de Verzekerde:

- Veiligheidssoftware en controles (zoals antivirus) heeft op zijn IT-systemen en hardware, dewelke op regelmatige basis wordt geupdate.
- Toegangscontroles heeft voor personeel en andere personen die toegang nodig hebben ("privileged acces") tot gevoelige data.
- Back-up en recovery procedures heeft voor mission critical systemen, data en informstie die nodig zijn voor de werking van zijn kantoor.
- Maandelijks zijn IT-systemen en applicaties scant en patched.
- Minstens jaarlijks haar werkgevers opleidt met betrekking tot 'best practices' inzake cyberveiligheid.
- Geen gebruik maakt van software dat niet langer verkocht, beveiligd of ondersteund wordt door de ontwikkelaar.
- Om de 2 maanden haar paswoorden wijzigt.
- Maximum 15% van zijn omzet haalt uit activiteiten in de Verenigde Staten/Canada.
- Op het ogenblik van ingang van de polis geen kennis heeft van omstandigheden die tot een vordering of administratief onderzoek (Privacy commissie) kunnen leiden ten gevolge van het verlies of vrijgeven van vertrouwelijke informatie.

# Door verzekeraar opgelegde beveiligings-maatregelen

Bijkomende dekking mbt cyberdiefstal

Indien er klaarblijkelijke interne instructies ter betaling van meer dan 10.000 EUR, en/of gewijzigde betalingsinstructies worden gegeven, dan is de dekking cyberdiefstal enkel verworven mits er een call is naar het telefoonnummer van diegene die de instructie gaf, waarbij dit telefoonnummer :
a/ hetzij in het dossier van de verzekerde werd bijgehouden, of
b/ opgenomen is in een intern telefoonboek van de verzekerde, of
c/ publiek beschikbaar is.

# Conclusies

- Ongevallenvoet per advocaat relatief laag.
- Gemiddelde kost per schadedossier stijgt
- Grootste financiële impact Cybertheft, Business mail compromise, Ransomware.
- Business mail compromise beperkt, hoogste frequentie, 22 dossiers.
- Aandacht voor voldoende beveiliging voorzien, gebruik double authentification, dubbel check rekeningnummers.

# Vragen?